

Title

Method for Making Secured Personal Identity Card and Procedures for Validation and Obtaining Secure Personal Information

Cross Reference

- 5 This is a regular application of a provisional application, application number 60/193,950, filed on March 31, 2000.

Background of the Present Invention

Field of Invention

- 10 The present invention relates to method of making an identity card, and more particularly to a method for making a secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, which can precisely distinguish an individual's identification and securely protect the privacy of the individual.

Description of Related Arts

- 15 Nowadays, an identity card is commonly used in order to identity ourselves. The identity card which contains personal information is easy to be stolen and used since the procedure of verification of the identity is simple and not secured. Usually, the identity card has a predetermined PIN as a password containing different combinations of numbers is provided for a user to identity himself or herself. The identity card contains
20 the user's general personal data, such as his/her name, photo or blood type, that is easy to be duplicated or modified.

- In order to verify the user identification, the predetermined PIN is usually used such that an input PIN is matched to the predetermined PIN preset in the identity card. However, the PIN can be stolen easily by releasing it to someone or decoded by the
25 computer. So, someone can enter our lives without permission by using our personal

information and, worse, our personal information may get changed and we may get in trouble by someone inputting any unwanted data into the identity card. In such conditions, people may lack security of the society.

Summary of the Present Invention

5 A main object of the present invention is to provide a method for making a secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, wherein the identity of the individual is secured since the verification requires personal information, such as fingerprints, that is unique and cannot be copied and replaced.

10 Another object of the present invention is to provide a method for making a secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, wherein additional security can be added to guard against the forced entry such that various biometrics information can be used for different transactions or difference levels of security.

15 Another object of the present invention is to provide a method for making a secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, which can be used to guarantee personal privacy. By using selective information such as PIN or biometrics information, an individual can protect his/her name or photo or other chosen information
20 concerning his/her identity from others when dealing with his/her confidential subject matter. For example, when the identity card holder requests a DNA test for AIDS, he/she can give the PIN number to the laboratory for testing AIDS and then open his/her section of the identity file that only contains information according to his/her DNA data. Furthermore, the identity card holder can give instructions about the directory that he/she
25 wants to store the new testing data without releasing the unwanted information. The people in the laboratory will not know whose DNA and whose file number (PIN) correspond to this sample. The activation procedure in this example can be as simple as taking a fingerprint in a recording device that provides the password.

Another object of the present invention is to provide a method for making a secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, wherein the unique personal biometrics information is used such that the authenticity is guaranteed.

5 Another object of the present invention is to provide a method for making a secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, wherein data at the lowest level of security such as name, sex, and age can be made available for general purpose or for community population statistical analysis, daily information etc without breaching the
10 privacy act. These data can be stored in the section of the identity file that are deemed by society as non-critical will be released to the government or anyone deemed necessary without the need of an activation procedure of the file by the individual concerned. For example, the information in such section may contain an ID number or Social Security number that issued by the government.

15 Accordingly, the information contained in an identity card for a person forms an identity file that consists of the name, the photo, the signature, as well as biometrics information such as the fingerprint, the iris pattern and possibly more detailed information on the DNA sample from the person. This file can be compressed and be given a code, used as the PIN for the individual to whom the information belongs. When
20 the information is required for the verification of the identity of this person, he/she must provide the PIN as well as taking certain specific procedures, such as having his/her fingerprint taken, in order to activate the decoding process of the file. Thus, even if someone knows the PIN, the privacy of the individual is protected unless he/she cooperates by providing the biometrics information.

25 This has several advantages compared to existing identity cards. First of all, the identity of the individual is secured unless he/she cooperates by following specific procedure of opening up the file for verification. Different procedures correspond to different sections of the file to be opened.

30 For example, how can an individual protect his/her name or photo or other chosen information concerning his/her identity from others while requesting a DNA test for AIDS? We provide the following method. He/she can first give the PIN number to the laboratory for testing AIDS and then activate the opening procedure of his/her identity

file the section that contains ONLY his/her DNA information. The people in the laboratory will not know whose DNA and whose file number (PIN) correspond to this sample.

The activation procedure in this example can be as simple as taking a fingerprint in a recording device that provides the password. Testing of relationship between parents and child can also be made in a similar way, provided that all three parties involved activate the DNA section of the corresponding files and authorize the laboratory to read in the data and perform the DNA diagnostic test on the relationship.

However, the laboratory technicians will only see a set of three PIN's and three DNA data files, without any knowledge or ability or authority to identify the individuals corresponding to these files. There will also be no 'big brother' in the government in the sense that only those sections of the identity file that are deemed by society as non-critical will be released to the government without the need of an activation procedure of the file by the individual concerned.

For example, this can be a section that is contained in present day ID card or Social Security Card issued by the government. The method of making the identity file and the procedures for activation and verification are described in details below, with many practical applications afterwards.

The following items are the distinctive features according to the present invention:

1. Methodology of data collection for the identity file

1.1 The identity file consists of a number (n) of sections. Each section contains a particular class of information that can be used to identify the person.

The following classes are to be included:

1.1.1 Basic information appearing in existing identification card. This usually contains the name, the birthday, as well as some basic numbers such as social security number in USA, passport records ...etc. This class of information can be made available under local laws and upon request from the government.

1.1.2 Simple biometrics information that is standard, such as color of hair, eyes, and recent photograph.

1.1.3 Simple biometrics information that is less standard, such as iris pattern, fingerprints, and hand prints.

5 1.1.4 Standard biometrics information that is related to the medical record of the person.

1.1.5 DNA fingerprint and other such information of the person

1.1.6 Voice recording of the person of a selection of standard messages.

1.1.7 Any other records deem important to the person who wishes to put in.

10 1.1.8 In the cases of the need of authentic sampling such as Human ID testing. Sampling procedure can also be securely monitored, with the help of the third party such as Notary Public or Attorney; the use of real time internet recording and sending of data for testing. (you can think of new classes here.)

15 1.2 Using existing multimedia data management, the sections of 1.1 are to be converted into standard files with appropriate file types.

1.3 Using a selection of data compression techniques, each section files is to be compressed and a header is added to form the PIN number for that section. The header, which is the PIN number of an individual section, consists of five pieces of information:

20 1.3.1 The section identification number to be assigned based on a random number generator. The range of the section identification number can be fixed to run from 00 to 99, if there are not more than 100 sections in the identity file.

25 1.3.2 In order to classify the level of confidentiality of the section, a digit is appended onto the section identification number. For example, when there are three levels of confidentiality, the digit can be 1, 2, and 3. If the section is not confidential, the digit 0 is assigned.

1.3.3 The method of data compression, chosen from a selection of methods using a random number generator. This can be an integer.

1.3.4 The file type from a selection of types using a second random number generator. This is the second integer.

5 1.3.5 An integer to denote the status of the section.

For example, if the section file is non-confidential, then we denote it with 0. If the section is confidential, it is given a nonzero integer. To give a simple example, let there be only three modes of biometrics information considered, namely fingerprint, iris pattern and voice recording. We can order them from 1 to 3, with 1 corresponding to fingerprint, 2 for iris pattern, and 3 for voice recording. (Example 1: the section header (or section PIN) for 120520 means that this is the 12 section, of level of confidentiality 0, compressed with method 5, and of file type 2, and is of non-confidential status.

10

Example 2: the section header for 022331 means that this is the 02 section of level of confidentiality 2, compressed with method 3, and of file type 3, and required the fingerprint to open this file.)

15

1.4 A special section called the K section, contains the encrypted data corresponding to the biometrics information used in the authorization process. In the above example, this K section contains the fingerprints, the iris pattern and voice recording. This section requires the use of public key encryption technology for its opening. The public key is also used as the personal password for the entire identity file. When K section is opened, one cannot view the information inside, but can compare overlap of information input with the stored information in K section. Therefore, K section will be used for verification purpose of biometrics information only.

20

1.5 The entire collection of section files, with their corresponding PIN's, form the encrypted code for the identity file. The PIN for the entire identity file is formed using the following procedure.

25

1.5.1 For the given n sections of the identity file, choose a random number generator to generate a sequence of n digits to denote the ordering of the sections. This

sequence of n digits, denoted by X, forms the master PIN number for the entire identity file. X is to be remembered by the identity card holder.

1.5.2 An image sequence of n digits, denoted by Y, is to follow X. Y contains the mode of biometrics information for the corresponding section in X.

5 1.5.3 The entire identity card number will be denoted by XY and a bracket (), which value consists of two digits to be keyed in by the identity card holder.

(For example, consider that there are 5 sections of the entire identity card. X can then be 43152. This identity card number means that the section ordering is first the fourth section, then the third section, then the first section, then the fifth section and then the second section. Supposing that we have section 1 as non-confidential, section 2,3, and 4 are confidential and requires respectively the supply of biometrics information of the fingerprint, the iris pattern and again the fingerprint for the opening of the section, and finally section 5 is non-confidential. Then the corresponding Y is 01210. The PIN number of this identity file is 4315201210. If the bracket () contains the digits 03, then
10 the identity cardholder wants to open up section 3.)
15

1.5.4 One can also use other method for the coding of X. The main idea is that X is some password that is used to open the identity file using public key. The opening of the identity file consists of the following two features: (1) the non-confidential section can be opened. (2) the K section is opened not for viewing, but only for the verification purpose of other confidential sections.
20

The following introduces a method of activation of a section of the identity file. The activation process of a section file is defined to be the authorization process of opening a file after the verification of the PIN of that entire identity file.

2.1 The verification of the PIN of the entire identity file consists of the
25 following steps:

2.1.1 The identity card holder will key in his/her PIN number for the entire file, excluding the last two digits in bracket. If the PIN is correct, then the cardholder will be authorized to proceed further.

2.1.2 The last two digits are to be supplied by the identity card holder to indicate which section file is to be opened.

2.1.3 If the section file does not require a key to be opened, (as indicated in 1.3.4), then the section file will be opened.

5 2.1.4 If the section file requires a key to be opened, then the cardholder must supply the appropriate biometrics information to open the section file. In the above example, when section 3 is to be opened, the cardholder must provide his/her iris pattern. When the cardholder provides the correct iris pattern that matched the K section of the identity file, section 3 will be opened.

10 2.2 Information released consists of the opened section files and the file number of the identity card. Therefore, there is complete privacy unless there is a release of both the personal file containing the name, photographs etc of the person and the confidential section. This can be prevented by a security procedure discussed in 3.

3. Applications and security of the identity card The identity card holder has
15 the freedom to release his personal identity including his confidential section files by supplying the correct PIN as well as the appropriate biometrics information. However, there is always a protection from threatening situation where the person is forced to release all section information, while an emergency signal is sent simultaneously to destined location for help. This is achieved by a particular combination of biometrics
20 information. For example, if the K section is to be opened under normal situation, i.e., not under threat, then the cardholder will supply his fingerprints of the thumb and the index finger. On the other hand, if the cardholder is under threat, how can he/she comply with the threatening party and send a distress signal to a helping party simultaneously? In this situation, the cardholder can supply the finger print of his thumb which will authorize the
25 opening of the appropriate section by checking the K section, as well as the finger print of his little finger. Which particular choice of fingers to be used by the cardholder is only known to the cardholder. As a result, the threatening party will have no way to know whether a distress signal has been sent, because in both cases, the finger print of the thumb already authorize the opening of the appropriate confidential section. The full
30 protection of the information in the identity file is provided by the definition of the corresponding modes of biometrics information for the sections and the memorization of these modes by the identity cardholder. In the above example, the code Y must be

memorized in addition to the meaning of 1 for fingerprint, 2 for iris pattern and 3 for voice recording. Furthermore, in order to have the ability to send signals for help, a special fingerprint, for example the little fingerprint, must be remembered as a mode for the sending of distress signal.

5 4. Example of operation

4.1 General operation:

First, the identity card holder will have his personal information taken as defined in section 1.

10 Next, he will have to choose the mode of biometrics information for verification. For example, he will decide that he only use fingerprints and iris pattern. He should also decide at the same time the mode of distress signal. For example, he will use the right thumb and the left thumb for normal opening of a confidential section, but will use the right thumb and right index finger for the opening of the confidential section while sending a signal for help to the police. This decision must be memorized.

15 Finally, he will designate which section file will be confidential, and if so, what is the mode of biometrics information required for its opening. He will form the PIN of his identity card by providing X and Y. Y is used as a string of reminder for the mode of biometrics information required for the opening of the confidential section. An outsider will not be able to interpret the mode even if the outsider understands the method of PIN
20 generation.

4.2 Secure and authentic sampling for personal bio-testing (e.g. Blood, urine etc. including DNA)

25 In the case of forensic or paternal DNA identification, the authenticity of the sample must be absolutely certain. Using the above scheme and the real time internet communication, the processes of sampling and transportation can be made securely. The person to be tested can activate his own file. The sample taking process is recorded with a video-equipped computer. His personal ID encrypted data (or bar code) is placed onto the sample. If testing must be done in another laboratory, the sampling (video recording process, etc.) data is immediately transmitted to his personal data file and only the

required information is sent to the testing center. The results will be automatically recorded into his data file only with the given encrypted ID without revealing his real personal information so that absolute privacy is ensured. If required, he will then activate his file accordingly for whatever purpose he desires OR is required by proper authority upon his cooperation. This procedures will then ensure the authenticity. Utilizing the internet this can be done anywhere else.

Brief Description of the Drawings

Fig. 1 is a block diagram of a method for making a secured personal identity card according to a preferred embodiment of the present invention.

Fig. 2 is a block diagram of procedures for validation and obtaining secure personal information according to the above preferred embodiment of the present invention.

Detailed Description of the Preferred Embodiment

Referring to Figs. 1 and 2 of the drawings, the present invention provides a method for making secured personal identity card and procedures for validation and obtaining secure personal information, including medical and/or DNA data, are illustrated, which comprises the steps of making secured personal identity card and the steps of validation and obtaining secure personal information, wherein the steps of making secured personal identity card, as shown in Fig. 1, as follows:

(1) Collect personal information for creating an identity file wherein the identity file comprises a plurality of sections each comprising a particular class of information that adapted to be used to identity a person selectively.

(2) Preset a header PIN number for each section for representing the header of each section wherein each header PIN number comprises a section identification number, a section confidential number, a data compression number, a file type number, and a section status number.

(3) Create a distinctive section comprising an encrypted data corresponding to biometrics information used in an authorization process.

(4) Preset a master PIN number for the identity file wherein the master PIN number comprises an ordering of the sections.

5 The steps of validation and obtaining secure personal information, as shown in Fig. 2, as follows:

(5) Input a PIN number by an identity card holder.

(6) Compare the inputting PIN number with the preset master PIN number.

10 (7) Open a respective section of the identity file indicated in the input PIN number.

In step (1), the personal information collected from a person is saved in the particular classes of the sections, wherein the personal information comprises:

15 (1.a) Basic information appearing in existing identification card such as the name, the birthday, as well as some basic numbers such as social security number, passport records, etc, wherein the class of information can be made available under local laws and upon request from the government.

(1.b) Simple biometrics information that is standard, such as color of hair, eyes, and recent photograph.

20 (1.c) Simple biometrics information that is less standard, such as iris pattern, fingerprints, and handprints or any other proven forms.

(1.d) Standard biometrics information that is related to the medical or genetic record of the person.

(1.e) DNA fingerprint, sequence profile and other such information of the person.

(1.f) Voice recording of the person of a selection of standard messages.

(1.g) Any other records deem important to the person who wishes to put in.

5 In the cases of the need of authentic sampling such as Human ID testing, Sampling procedure can also be securely monitored, with the help of the third party such as Notary Public or Attorney; the use of real time internet recording and sending of data for testing. Such security measures can be coupled with door key passes that are provided by a separate security company with internet time monitoring system.

The step (1) further comprises the steps of:

(1-1) Convert the identity file into a standard readable form.

10 (1-2) Compress the identity file for minimizing a volume thereof.

In step (1-1), after the personal information is collected, the identity file is converted into a standard readable file type by an existing multimedia data management, wherein the identity file is then compressed into a compact size thereof, in step (1-2), and stored in a data base system such as computer or ISP server. The advantage of
15 compressing the identity files is that more identity files can be stored in the data base system by reducing its size without corrupting or damaging the personal information inside the identity file.

In step (2), the header PIN number is preset for each section as a reference wherein each header PIN number is combined with five corresponding informative
20 numbers, which are the section identification number, the section confidential number, the data compression number, the file type number, and the section status number

The section identification number is a number for distinguishing each section in the identity file, which is assigned based on a random number generator. For example, the range of the section identification number can be fixed to run from 00 to 99, if there
25 are not more than 100 sections in the identity file. Also, alphanumeric characters can also be used if desired by local authorities.

In order to classify the level of confidentiality of the section, a digit is appended onto the section confidential number. For example, when there are three levels of confidentiality, the digit of the section confidential number can be 1, 2, and 3 respectively. If the section is not confidential, the digit 0 is assigned to the section confidential number.

The data compression number indicates a method of data compression, which is chosen from a selection of methods by using a random number generator wherein the data compression number can be an integer.

The file type number indicates what selection of type of the identity file is belonged to, which is generated by using a second random number generator. The file type number is a second integer.

The section status number, which is an integer, denotes the status of the section of the identity file which is the mode of the biometrics information. In other words, each nonzero integer of the section status number denotes one mode of the biometrics information is required in order to open the identity file.

For example, if the section in the identity file is non-confidential, then it is denoted with zero. If the section is confidential, it is given a nonzero integer. To give a simple example, consider that there are only three modes of biometrics information, which are fingerprint, iris pattern and voice recording and are being ordered from 1 to 3, with 1 corresponding to fingerprint, 2 for iris pattern, and 3 for voice recording respectively. When the section header, i.e. the header PIN number, is numbered as 120520 that denotes the section identification number is 12, the section confidential number is 0, the data compression number is 5, the file type number is 2, and the section status number is 0. So, the header PIN number means this is the section 12, the level of confidentiality is 0, the method of compression is 5, the file type is 2, and this is a non-confidential status which does not require any biometrics information. For another example, the section PIN number (the section header) is numbered as 022331 that denotes the section identification number is 02, the section confidential number is 2, the data compression number is 3, the file type number is 3, and the section status number is 1. So, the header PIN number means this is the section 02, the level of confidentiality is 2, the method of compression is 3, the file type is 3, and it is required the fingerprint to open this file.

In step (3), the distinctive section comprises the encrypted data corresponding to the biometrics information used in the authorization process. In the above example, the distinctive section comprises the fingerprints, the iris pattern and voice recording. The distinctive section requires the use of master key encryption technology for its opening wherein the master key is also used as the personal password for the entire identity file. When the distinctive section is opened, one cannot view the information inside, but can compare overlap of information input with the stored information in the distinctive section. Therefore, the distinctive section will be used for verification purpose of biometrics information only.

The step (4) further comprises the step of:

(4-1) Create an identity card number which comprises the master PIN number, a mode of biometrics information for each corresponding section, and a section number.

In step (4), after collecting the entire sections of the identity file with the respective header PIN number thereof, the master PIN number, which comprises an ordering of the section, is provided for the identity card holder wherein the identity card holder is able to use the master PIN number to verify himself/ herself and activate the sections in the identity file.

The ordering of the sections is denoted as a section order number which is a sequence of the section number. In other words, for given n sections of the identity file, a sequence of n digits is generated by a random number generator to denote the ordering of the sections. The sequence of n digits of the section order number is partially formed into the master PIN number for the entire identity file, which is needed to be memorized by the identity card holder.

In step (4-1), the mode of biometrics information for each corresponding section is denoted by a sequence of digits of a biometrics mode number which is followed by the section order number in the master PIN number. Furthermore, the section number, which is formed by two digits for the identity file holder to input, denotes which desired section of the identity file that the identity card holder want to be opened up.

For example, there are 5 sections of the entire identity file and are ordered to be 43152 as the section order number, the first section ordering is the fourth section, then the

third section, then the first section, then the fifth section and the last section ordering is the second section. Supposing that the section 1 as non-confidential, section 2, 3, and 4 are confidential and require a mode of biometrics information of the fingerprint, the iris pattern and again the fingerprint for the opening of the section respectively, and final
5 section 5 is non-confidential. Then the corresponding biometrics mode is 01210. The identity card number of this identity file is 4315201210. If the section number is input as 03, it means that the identity card holder wants to open up section 3.

One can also use an alternative method for the coding of section order number. The main object of the section order number, which acts as a password, is used to open
10 the identity file as the master key that mentioned above. The master PIN number consists of the following two features: (1) Only the non-confidential section can be opened, i.e. not biometrics information is required to be verified. (2) The distinctive section cannot be opened for viewing the personal information therein, but only for the verification purpose of other confidential sections.

15 In step (5), the identity card holder is guided to key in his/her master PIN number for the identity file. The identity card holder must input the master PIN number provided in step (4) in order to process the activation of a section and the authorization of opening the identity file.

The step (6) further comprises a step of:

20 (6-1) Input a section number that the corresponding section of the identity file is desired to be open by the identity card holder.

In step (6), after comparing the inputting PIN number with the master PIN number, if the input master PIN number is correct, then the identity card holder will be authorized to proceed further.

25 In step (6-1), after matching the master PIN number, the identity card holder is then guided to input the section number with respect to the section that the identity card holder want to open wherein the section number is formed by two digits.

If the desired section does not require any biometrics information to open, wherein the section status number of the header PIN number is denoted as 0 in step (2), the desired section will be opened.

5 If the desired section requires biometrics information to open, wherein the section status number of the header PIN number is denoted as nonzero in step (2), the corresponding biometrics information is needed to be provided to open the section of the identity file. In the above example in step (4), when section 3 is desired to be opened, the identity card holder must provide his/her iris pattern. When the identity card holder provides the corrected iris pattern that matched the distinctive section of the identity file,
10 section 3 will be opened.

Moreover, information released comprises the opened section files and the file number (header PIN number) of the identity card, which must be different from the master PIN number of the entire identity file. Therefore, there is complete privacy unless there is a release of both the personal files containing the name, photographs etc of the
15 person and the confidential section.

The present invention further comprises a default step of:

(8) Send a distress signal when a distress code is detected.

20 The identity card holder has the freedom to release his personal identity including his confidential section files by supplying the correct master PIN number as well as the appropriate biometrics information. However, there is always a protection from threatening situation where the person is forced to release all section information, while an emergency signal is sent simultaneously to destined location for help.

25 In step (8), the distress code is preset by the identity card holder in step (4) wherein the distress code is combined with the master PIN number and a biometrics information such that when the identity card holder input the master PIN number and the respective biometrics information, the distress code is then activated and the distress signal is sent to a destined location such as police station for help.

The distress code is achieved by a particular combination of biometrics information. For example, if the distinctive section is opened under normal situation, i.e.,

not under threat, then the identity card holder will supply his fingerprints of the thumb and the index finger which are the required biometrics information with respect to the section. On the other hand, if the identity card holder is under threat, how can he/she comply with the threatening party and send a distress signal to a helping party simultaneously? In this situation, the identity card holder can supply the finger print of his thumb which will authorize the opening of the appropriate section by checking the distinctive section, as well as the finger print of his little finger which is the distress code preset by the identity card holder. The particular choice of fingers to be used as the distress code is only known by the identity card holder. As a result, the threatening party will have no way to know whether the distress signal has been sent, because in both cases, the finger print of the thumb already authorize the opening of the appropriate confidential section. The full protection of the information in the identity file is provided by the definition of the corresponding modes of biometrics information for the sections and the memorization of these modes by the identity card holder. In the above example, the biometrics mode must be memorized in addition to the meaning of 1 for fingerprint, 2 for iris pattern and 3 for voice recording. Furthermore, in order to have the ability to send signals for help, a special fingerprint, for example the little fingerprint, must be remembered as a mode for the sending of distress signal.

In order to operate the present invention, the personal information of the identity card holder will be collected in step (1). Next, he will have to choose the mode of biometrics information for verification. For example, he will decide to use fingerprints and iris pattern only. He should also decide the distress mode at the same time. For example, he will use the right thumb and the left thumb for normal opening of confidential section and will use the right thumb and right index finger for the opening of the confidential section for activating the distress code and sending the distress signal for help. The distress code must be memorized in order to prevent the distress signal from being sent unintentionally or disabled while in danger.

Furthermore, the identity card holder will designate which section file will be confidential for setting the master PIN number, and if so, what is the mode of biometrics information required for its opening, so as to preset the biometrics mode number. The biometrics mode number is used as a string of reminder for the mode of biometrics information required for the opening of the confidential section. Outsider will not be able to interpret the mode even if the outsider understands the method of PIN generation.

The present invention is also adapted to operate the secure and authentic sampling for personal bio testing such as blood, urine etc. used for bioassays, including DNA. In the case of forensic or paternal DNA identification, the authenticity of the sample must be absolutely certain. Using the above scheme and the real time Internet communication, the processes of sampling and transportation can be made securely. The identity card holder, who is being tested, can activate his own file at first. The sample taking process is then recorded by video equipped with computer. His personal identity encrypted data (or bar code or fingerprints etc) is placed on the sample for individually identification. If the test must be done in another laboratory, the sampling (video recording process etc) data is immediately transmitted to his personal data file and only the required information is sent to the testing center. The results of the test will be automatically recorded on his data file only with the given encrypted data without revealing his real personal information so that the absolute privacy is ensured. If required, he will then activate his file accordingly for whatever purpose he desires or as required by proper authority upon his cooperation. These procedures will then ensure the authenticity. Preferably, by utilizing the Internet, the process can be done anywhere even the identity card holder is out of his country.